National Aeronautics and Space Administration

The Great Wave of Reform: The Prophetic Fallacy of the Fukushima Daiichi Meltdown

Steve Lilley

10/15/2015

Background

- March 11, 2011, off the Pacific coast of Tōhoku, Japan: At 2:46 p.m. Japan Standard Time (JST), a magnitude 9.0 earthquake occurred 43 miles east of the Oshika Peninsula. The earthquake generated 133-foot tsunami waves that travelled 6 miles into mainland Japan. According to the latest accessible Japanese National Police Agency police reports, the earthquake and tsunami are responsible for 15,891 dead, 6,152 injured, and 2,584 missing peoples. In addition to the horrific loss of life, 129,290 buildings have been reported collapsed, with another 1,020,777 structures sustaining varying degrees of damage. The disaster also triggered the Fukushima Daiichi Nuclear Power Plant accident—the second Level 7 incident on the International Nuclear Event scale.

The Fukushima Daiichi Catastrophe

- Analysis of the safety history of Fukushima Daiichi reveals a catastrophic failure of prediction on behalf of the plant’s Tokyo Electric Power Company (TEPCO) management. How could planners overlook the tsunami?

Hazards of Predicting the Future

- In 1962, Arthur C. Clarke, published the essay, “Hazards of Prophecy,” which covered the two traps of assumptions: “failures of nerve” and “failures of imagination.” Failure of the imagination manifests when known facts are respected but vital truths are still unknown, and the possibility of the unknown (the unknown unknowns) is not confessed. Failure of nerve, the more common fallacy occurs when given all the facts, the inescapable conclusion is not seen.

What Happened

- The seismic activity of the Great East Japan Earthquake forced the emergency shut-down feature on reactors 1, 2, and 3. Off-site electricity to the power plant was also disrupted by the tremors and backup power was tapped from a 66kV transmission line from the Tohoku Electric Power Company Network. However, the back-up line failed to power reactor 1 due to a mismatched circuit connection.
- At 3:17 p.m. JST, tsunami waves flooded and destroyed the emergency diesel generators at the complex. Seawater cooling pumps and electric wiring system for the DC power supply for reactors 1, 2, and 4 failed shortly after. All power was effectively lost except for emergency diesel generator power to reactor 6.
- Without power, the operators worked tirelessly to monitor and cool the overheating reactors, at one point salvaging car batteries from destroyed vehicles to power necessary equipment. Hydrogen explosions from emptying coolant reservoirs led to interruptions in the recovery operations, which failed when the Unit 2 reactor suppression chamber failed and discharged radioactive material.

excellence • teamwork • safety • integrity • knowledge

Proximate Cause

- The loss of electric power after flooding made it difficult to effectively cool down the reactors in a timely manner. Cooling and observation were heavily dependent on electricity for coolant injection and depressurization of the reactor and containers, and removal of decay heat at the final heat-sink. Lack of access due to the disaster obstructed the delivery of necessities like alternative seawater injection via fire trucks.

Underlying Issues

- The Nuclear Accident Independent Investigation Commission (NAIIC), formed on October 30, 2011 to investigate the direct and indirect causes of the Fukushima accident, was the first independent commission created in the history of Japan's constitutional government. In its legal investigation, the NAIIC concluded that "the disaster was man-made and the result of collusion between government, the regulators, and TEPCO, and a lack of governance by said parties," citing that the organizational and regulatory systems supported faulty rationales for decisions and actions.

Debris from the upper levels of Unit 4 lies beside the building. Source: IAEA

Disregard of Regulations

- 1967 constructions plans for the Fukushima Daiichi isolation condenser deviated from the original reactor plans submitted to the government in 1966. The changes were not reported in violation of regulation. TEPCO’s configuration control was scrutinized in February 2012 by Japan’s Nuclear and Industrial Safety Agency (NISA). NISA requested explanation by March 12, 2012; however, TEPCO, unable to supply an official explanation.
- In 2002, employees of General Electric (GE), the reactor designer, reported to the Japanese government that TEPCO injected air into the containment vessel of reactor Number 1 to artificially lower the rate of a leak. The scandal, in addition to a fuel leak at Fukushima Daini, forced TEPCO to temporarily shut down all 17 reactors. Falsified safety records and inspections in conjunction with the number 1 unit dating back to 1989 were revealed by other GE employees. Contractors admitted to falsifying reports at the request of TEPCO. Further disclosures implied that GE ignored warnings of major design failings from members of its contract staff (who resigned in protest of negligence) in 1976.

Poor Safety History

- December 29, 2011, TEPCO officials admitted to events occurring in 1991, where one of two backup generators for Number 1 failed after it was flooded with seawater leaking into the turbine building from a corroded seawater cooling pipe. **Superiors were informed about the accident, and of the possibility that a tsunami could inflict similar damage to the generators in the turbine-buildings near the sea.** In lieu of moving the generators to higher ground, TEPCO installed leak-proof doors in the generator rooms.
- According to the NAIIC, regulators and TEPCO were aware of the risk that a total loss of electricity at Fukushima Daiichi would occur if flooding from a tsunami were to reach the level of the site since 2006, and that they were doubly aware of a risk of reactor core damage from loss of seawater pumps in the case of tsunami waves over 10 meters high. The NISA understood the TEPCO had not taken any protective or mitigating measures, but did not provide instructions to TEPCO to do so.

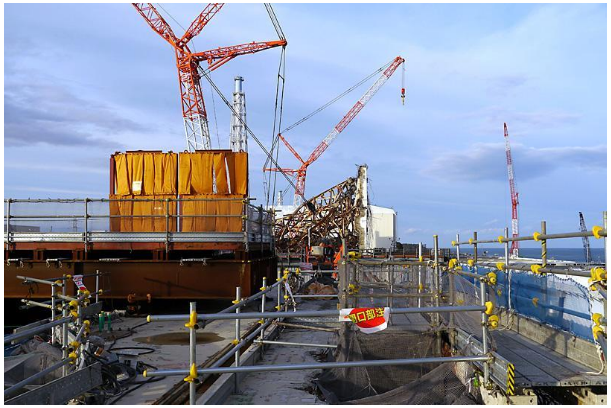
Workers in protective clothing and masks outside the Emergency Response Centre, the main control hub at the Fukushima Daiichi site. Source: IAEA

Lack of Response to Natural Disaster Concerns

- A 2008 study performed by TEPCO’s nuclear supervisory department concluded that there was an immediate need for improved seawater flooding protection. The study mentioned the threat of tsunami waves over 10 meters tall. Executives dismissed the perceived risk as unrealistic; concluding that, even when presented with historical data, there was a failure to imagine that such conditions would recur.
- In 2008, The International Atomic Energy Agency (IAEA) cited that an earthquake of a 7.0 or higher magnitude posed a serious threat at a G8 Nuclear Safety and Security Group assembly.
- On 2 October 2011, the Japanese Government released a TEPCO report that proved TEPCO was aware of the possibility that the plant could be hit by a tsunami with waves far higher than the designed 5.7 meters buffer. Simulations based on the1896-earthquake in this area, revealed the likelihood of waves between 8.4 and 10.2 meters capable of flooding the site.
- No mitigation was planned before October 2012.
- In contrast, the Tokai Nuclear Power Plant protective dike was raised to 6.1 meters after simulations showed the possibility of higher than expected tsunami waves. Even unfinished at the time of the March 11, 2011 tsunami, he dike protected two seawater pumps and emergency diesel generators and allowed for the reactor to be kept in cold shutdown even though external power was lost.

Aftermath

- The Nuclear Safety Commission Chairman stated in February 2012 that, “Japan’s atomic safety rules are inferior to global standards and left the country unprepared for the Fukushima nuclear disaster last March.” There were flaws in, and lax enforcement of, the safety rules governing Japanese nuclear power companies, and this included insufficient protection against tsunamis.
- The NAIIC made recommendations pertaining to the creation of a permanent committee to deal with issues regarding nuclear power in order to supervise regulators and provide security to the public. The committee should be
  - Responsible for conducting regular investigations and explanatory hearings of regulatory agencies, academics, and stakeholders
  - Responsible for establishing an independent advisory body to stay abreast of industry and government dealings; transparent in decision making processes to the national government and exclude involvement of stakeholders in decision making; technically proficient in nuclear technology.
- The NAIIC made recommendations pertaining to the reforming of energy laws to adhere to global standards, including the monitoring of operators and backfit of outdated reactors.



A view from the top of Unit 4. The metal and rubble in the middle distance is the top of Unit 3, where cranes have to clear the debris remotely because of high radiation levels. Source: IAEA

Relevance to NASA

- Planners used of a narrow slice of historical data when estimating the risk of initiating event which contributed to a failure of imagination that a tsunami could overcome the break wall. Beyond the multiple failures on behalf of TEPCO and Japanese nuclear regulatory agencies, the critical question remains of when to draw the line—when safe is safe enough—in the design basis process.
- Teams with diverse viewpoints and broad, deep experience can overcome individual cognitive biases that can carve a path toward failure of imagination from the very beginning. Policy checks and balances on teams, such as NASA technical and safety requirements, are only as effective as the accountability behind them and depend upon how well both operators and regulators understand the technical basis behind such requirements.
- Sometimes the rationale behind a requirement stems from the context surrounding a failure. If the rationale is lost to history, it can rob a team of the technical argument (and nerve) to defend safety margins.
- Perhaps harder to overcome is the instance when a regulator itself places public safety below the business interests of a powerful industry. Safety hazards needing thorough mitigation can be perceived instead as business problems that demand efficiencies.
- As this case study comes to press, the first Japanese nuclear plant restart took place after a nationwide 48-plant shutdown in 2011. Effects of an historic wave of reform may become visible.

Storage tanks for contaminated water, a major challenge at the Fukushima Daiichi site. Source: IAEA

excellence • teamwork • safety • integrity • knowledge

NASA SAFETY CENTER